Van Ness Feldman LLP
vnf.com

Updated TSA Guidelines Suggest New Approach for Pipeline Cybersecurity

APRIL 24, 2018

Gwen Keyes Fleming and *Darshana Singh*

The Transportation Security Administration ("TSA") has released a newly updated version of its "Pipeline Security Guidelines" ("Guidelines") which outlines the measures that should be taken to protect pipeline cyber assets. TSA, which has oversight over more than 2.6 million miles of natural gas and oil pipelines, had not updated its Guidelines since 2011. However, the threat of cyberattacks on critical infrastructure sectors, including the energy sector, has increased in volume, sophistication, and magnitude over the last seven years. While the electric industry has binding and enforceable cybersecurity standards, the original Guidelines issued by TSA were not mandatory. The voluntary nature of the Guidelines has raised concerns for electric regulators, utilities, and lawmakers given the interdependent relationship between gas-fueled generation and the power grid. To bridge this gap, last month, the TSA refreshed its Pipeline Security Guidelines and, while the Guidelines are still not mandatory, they significantly bolster TSA's guidance with regard to cybersecurity measures.

Like the 2011 version, the revamped Guidelines are applicable to operational natural gas transmission pipeline systems, hazardous liquid pipeline systems, natural gas distribution pipeline systems, and liquefied natural gas facilities. However there are some key changes in this latest version. First, the incident response protocols have been changed. Second, the Guidelines take a new approach, which focuses on Operational Technology ("OT") systems and bifurcates the suggested measures based on whether an OT system is classified as a critical or non-critical pipeline cyber asset. Third, unlike the outdated 2011 guidelines, the TSA's Guidelines state that "to implement an effective cybersecurity strategy, pipeline operators should consider the approach" established by the National Institute of Standards and Technology ("NIST") in its recently updated "Framework for Improving Critical Infrastructure Cybersecurity" ("Framework"). Specifically, TSA's Guidelines outline suggested security measures by categories correlating with the main tenets of the voluntary NIST Framework. The TSA also encourages pipeline operators to look to the guidance issued by the Department of Homeland Security and the Department of Energy, as well as industry-specific standards and best practices when developing and implementing cybersecurity measures.

It is important to note that the most recent TSA Guidelines, like their predecessor, are mere guidance and do "not impose requirements on any person or company." However, as noted in a previous VNF Alert, this latest version reinforces the notion that implementing the NIST Framework is an important bell weather for critical infrastructure entities to undertake reasonable, pragmatic, and protective measures that can mitigate legal and technical risks. While it is unlikely that any mandatory regulations will be imposed on the natural gas industry in the near future, the recent cyberattacks within the gas sector have caught the attention of regulators, lawmakers, and interconnected energy sectors. The increasing pressure to impose mandatory guidance has placed pipeline operators under the microscope. It has become important, now more than ever, for operators to demonstrate that the voluntary standards are sufficient to provide the necessary level of cyber and by extension national security.

For more information

For assistance navigating the newly issued TSA Guidance along with existing guidance and industry standards, please contact Gwen Keyes Fleming, Darshana Singh, or any member of the firm's Cybersecurity practice at (202) 298-1800 in Washington, D.C. or in Seattle at (206) 623-9372.

Follow us on Twitter @VanNessFeldman